## **CLAIMS:**

1	1.	A method for organizing alerts into alert classes, both the alerts and alert classes		
2	having a plurality of features, the method comprising the steps of:			
3		(a)	receiving a new alert;	
4		(b)	identifying a set of potentially similar features shared by the new alert and one	
5	or more existing alert classes;			
6		(c)	updating a minimum similarity requirement for one or more features;	
7		(d)	updating a similarity expectation for one or more features;	
8		(e)	comparing the new alert with one or more alert classes, and either:	
9		(f1)	associating the new alert with the existing alert class that the new alert most	
10	closely matches; or			
11		(f2)	defining a new alert class that is associated with the new alert.	
1	2.	The method of claim 1 further comprising the step (a1) of passing each existing alert		
2	class 1	class through a transition model to generate a new prior belief state for each alert class.		
1	3.	A me	thod for organizing alerts having a plurality of features, each feature having one	
2	or more values, the method comprising the steps of:			
3		(a)	generating a group of feature records for a new alert, each feature record	
4	including a list of observed values for its corresponding feature;			
-5		(b)	identifying a set of potentially similar features shared by the new alert and one	
6	or more existing alert classes that are associated with previous alerts;			
7		(c)	comparing the new alert to one or more alert classes;	
8		(d)	rejecting a match if any feature for which a minimum similarity value has	
9	been set fails to meet or exceed the minimum similarity value;			
10		(e)	adjusting the comparison by an expectation that certain feature values will or	
11	will not match, and either:			
12		(f1)	associating the new alert with the existing alert class that the new alert most	
13	closely matches; or			
14		(f2)	defining a new alert class that is associated with the new alert.	

22

23

24

25

26

27

1

2

3

4

5

6 7

8

9

10

1

2

3

4

5

6

7

15	4. In an	intrusion detection system that includes a plurality of sensors, each of which	
16	generates alerts when attacks or anomalous incidents are detected, a method for organizing		
17	the alerts comprising the steps of:		
18	(a)	receiving an alert;	
19	(b)	identifying a set of features that may be shared by the received alert and one	
20	or more existing alert classes;		
21	(c)	setting a minimum similarity value for one or more features or feature group	

- (c) setting a minimum similarity value for one or more features or feature groups; comparing the new alert to one or more of the alert classes, and either:
- (d1) defining a new alert class that is associated with the received alert if any feature or feature group that has a minimum similarity value fails to meet or exceed its minimum similarity value; or
- (d2) associating the received alert with the existing alert class that the received alert most closely matches.
- 5. A method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, the method comprising the steps of:
  - (a) receiving a new alert;
  - (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;
  - (c) updating a minimum similarity requirement for one or more features;
  - (d) comparing the new alert with one or more alert classes, and either:
  - (e1) associating the new alert with the existing alert class that the new alert most closely matches; or
  - (e2) defining a new alert class that is associated with the new alert.
- 6. A method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:
- (a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;
  - (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;
    - (c) comparing the new alert to one or more alert classes;

10

11

12

- 8 (d) rejecting a match if any feature for which a minimum similarity value has 9 been set fails to meet or exceed the minimum similarity value, and either:
  - (e1) associating the new alert with the existing alert class that the new alert most closely matches; or
  - (e2) defining a new alert class that is associated with the new alert.